DaimlerChrysler AG

Patent Claims

1. A method for operating a vehicle in a mode of operation which can be activated by its user and which is restricted compared with a normal mode of operation of the vehicle, characterized in that the restricted mode of operation can only be deactivated again by an authorized person who does not need to be identical to the user.

2. The method as claimed in claim 1, characterized in that the restricted mode of operation is automatically restored even after the ignition has been switched off and the vehicle subsequently restarted, as long as it has not been deactivated again by the authorized person.

3. The method as claimed in one of the preceding claims, characterized in that the deactivation of the restricted operating mode is preceded by an authentication of the authorized person, wherein the person can authenticate him/herself particularly by the input of his/her fingerprint or a PIN number or via a central emergency service.

4. The method as claimed in one of the preceding claims, characterized in that the restricted mode of operation provides a restriction in the driving mode of the vehicle, particularly in the form of a predeterminable maximum speed and/or a maximum distance which can be traveled by the vehicle during the activation of the restricted mode of operation.

5. The method as claimed in one of the preceding claims, characterized in that the restricted mode of operation provides a restriction in the utilization of

the vehicle by the user, particularly in the form of a locking of the glove box and/or of the trunk of the vehicle.

6. The method as claimed in one of the preceding claims, characterized in that the restricted operating mode comprises a restriction in the access rights of the user to person-related data which are accessible via devices associated with the vehicle such as, for example, PC or navigation system.

7. The method as claimed in claim 6, characterized in that the restriction comprises a pure write protection for non-sensitive person-related data and a write and read protection for sensitive person-related data.

8. The method as claimed in claim 7, characterized in that the restriction provides an invariable initialization of devices of the vehicle such as, e.g. seats or entertainment devices, as determined by the non-sensitive person-related data of a predetermined person.

9. The method as claimed in one of claims 6 to 8, characterized in that during the deactivation of the restricted mode of operation by the authorized person, the person-related data of all persons affected are released again for reading and/or writing.

10. The method as claimed in one of claims 6 to 8, characterized in that during the deactivation of the restricted mode of operation by the authorized person, the person-related data of only individual persons, particularly of the authorized person him/herself, are released again for reading and/or writing.

11. The method as claimed in one of the preceding claims, characterized in that the range of the

restriction in the restricted mode of operation can be defined, in particular, by the user, preferably under menu control, haptically or by voice input.

12. A computer program with program code for a control device for operating a vehicle in a restricted mode of operation, characterized in that the program code is designed for performing the method as claimed in one of claims 1 to 11.

13. A data medium with a computer program as claimed in claim 12.

14. A control device (100) for operating a vehicle in a mode of operation which is restricted compared with a normal mode of operation, comprising the following:

a memory device (110) for storing the restricted mode of operation;
an input device (120) for activating the restricted mode of operation by the user of the vehicle and for deactivating the restricted mode of operation; and
a control device (140) for driving components (150-1...-N) of the vehicle for adjusting the mode of operation activated in each case;
characterized by an authentication device (130), which is constructed for ensuring that the restricted mode of operation can only be deactivated again by an authorized person via the input device (120).

15. The control device (100) as claimed in claim 14, characterized in that the input device is constructed for a manual or voice-controlled input, preferably under menu control.

16. The control device (100) as claimed in one of claims 13 to 15, characterized in that the input device (120) is constructed for reading-in biometric features,

particularly a fingerprint, and the authentication device (130) is constructed for comparing the biometric features read in with the biometric features of the authorized person with regard to a match.

17. The control device (100) as claimed in one of claims 13 to 16, characterized in that the input device (120) is constructed for reading-in a PIN number, and the authentication device (130) is constructed for comparing the PIN read in with a PIN allocated to the authorized person, with regard to a match.

18. The control device (100) as claimed in one of claims 13 to 17, characterized in that the authentication device (130) comprises a communication device (132) for performing the authentication by exchanging data with a service center.

19. The control device (100) as claimed in one of claims 13 to 18, characterized in that the memory device (110) is constructed separately from other memory devices, particularly from a memory device for the person-related data and preferably as a non-write-protected read-only memory.

20. The control device (100) as claimed in claim 19, characterized in that the type/the range of the restricted mode of operation stored in the memory device (110) can be changed via the input device (120).